Notice of Allowability	Application No. 09/657,122	Applicant(s) CHENG ET AL.
	Examiner Ronald Baum	Art Unit 2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *6/16/2004*.

2. ☒ The allowed claim(s) is/are *1,2,5-48 and 51-70*.

3. ☐ The drawings filed on _____ are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *07142004* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Robert Voigt, Jr., Reg. No. 49,159 on 7/14/2004.

1. Replace claims 25-46 with:

25. A virtual private network system comprising: a plurality of tunnels associated with a group name, wherein each of said plurality of tunnels associated with said group name comprises a plurality of nodes, wherein each of said plurality of nodes comprises a communication adapter to interconnect with said virtual private network, wherein one of said plurality of nodes is a server node, wherein one of said plurality of nodes is a client node, wherein said server node comprises: a group database, wherein said group database comprises said group name and a list of members associated with said group name; and a rules database, wherein said rules database associates said group name with a particular security policy, wherein said server node has a single copy of a security policy for each of the plurality of tunnels associated with said group name.

26. The virtual private network system as recited in claim 25, wherein said server node further comprises: a tunnel definition database, wherein a remote ID in said tunnel definition is defined as said group name, wherein said server node has a

single tunnel definition for each of the plurality of tunnels associated with said group name.

27. The virtual private network system as recited in claim 26, wherein a particular tunnel of said plurality of tunnels associated with said group name is activated, wherein said particular tunnel is associated with a particular member of said group name.

28. The virtual private network system as recited in claim 25, wherein said list of members associated with said group name comprise an ID type and an ID of each member associated with said group name.

29. The virtual private network system as recited in claim 28, wherein said ID type is an Internet Key Exchange (IKE) defined ID type, wherein said list of members is a non-contiguous list of IKE defined ID types.

30. The virtual private network system as recited in claim 28, wherein said ID is a login ID.

31. The virtual private network system as recited in claim 28, wherein said ID is a specified name.

32. The virtual private network system as recited in claim 26, wherein said tunnel definition database in said server node is configured by a user entering a local ID, a local ID type, said remote ID and a remote ID type through a GUI.

33. The virtual private network system as recited in claim 26, wherein said tunnel definition database in said server node is configured by a user entering a local ID,

a local ID type, said remote ID and a remote ID type through a command line interface.

34. The virtual private network system as recited in claim 25, wherein said group database in said server node comprises said group name and an ID type of each member of said group name and an ID of each member of said group name.

35. The virtual private network system as recited in claim 34, wherein said group database in said server node is configured by a user entering said group name, said ID type of each member of said group name and said ID of each member of said group name through a GUI.

36. The virtual private network system as recited in claim 34, wherein said group database in said server node is configured by a user entering said group name, said ID type of each member of said group name and said 1D of each member of said group name through a command line interface.

37. The virtual private network system as recited in claim 34, wherein said group database in said server node is configured by a user entering said group name, said ID type of each member of said group name and said ID of each member of said group name through configuration files.

38. The virtual private network system as recited in claim 25, wherein said rules database in said server node comprises said group name, a group name ID type and a security policy pointer.

39. The virtual private network system as recited in claim 38, wherein said rules database is configured by a user entering said group name, said group name ID type and said security policy pointer through a GUI.

40. The virtual private network system as recited in claim 39, wherein said rules database is configured by a user entering said group name, said group name ID type and said security policy pointer through a command line interface.

41. A virtual private network system comprising: a plurality of tunnels associated with a group name, wherein each of said plurality of tunnels associated with said group name comprises a plurality of nodes, wherein each of said plurality of nodes comprises a communication adapter to interconnect with said virtual private network, wherein one of said plurality of nodes is a server node, wherein one of said plurality of nodes is a client node, wherein said server node comprises: a group database, wherein said group database comprises said group name and a list of members associated with said group name; and a rules database, wherein said rules database associates said group name with a particular security policy, wherein said server node has a single copy of a security policy for each of the plurality of tunnels associated with said group name; wherein the server node further comprises; a tunnel definition database, wherein a remote ID in said tunnel definition is defined as said group name, wherein said server node has a single tunnel definition for each of the plurality of tunnels associated with said group name; wherein a particular tunnel of said plurality of tunnels associated with said group name is activated, wherein said particular tunnel is associated with a

particular member of said group name; wherein activating said particular tunnel comprises the steps of: sending a security policy stored in a policy database of said client node by said client node to said server node; sending a security policy stored in a policy database of said server node by said server node to said client node if said security policy stored in said policy database of said server node matches said security policy stored in said policy database of said client node; sending a first nonce by said client node to said server node; sending a second nonce by said server node to said client node; sending a first ID by said client node to said server node; and sending a second ID by said server node to said client node.

42. The virtual private network system as recited in claim 41, wherein said first and second nonce are used to generate key material for said server and client node, respectively.

43. The virtual private network system as recited in claim 41, wherein said policy database in said client and server node are configured by entering said security policy through a GUI at said client and server node.

44. The virtual private network system as recited in claim 41, wherein said policy database in said client and server node are configured by entering said security policy through a command line interface at said client and server node.

45. The virtual private network system as recited in claim 41, wherein said first ID is an ID of said particular member of said group name.

46. A virtual private network system comprising: a plurality of tunnels associated with a group name, wherein each of said plurality of tunnels associated with said group name comprises a plurality of nodes, wherein each of said plurality of nodes comprises a communication adapter to interconnect with said virtual private network, wherein one of said plurality of nodes is a server node, wherein one of said plurality of nodes is a client node, wherein said server node comprises: a group database, wherein said group database comprises said group name and a list of members associated with said group name; and a rules database, wherein said rules database associates said group name with a particular security policy, wherein said server node has a single copy of a security policy for each of the plurality of tunnels associated with said group name; wherein the server node further comprises; a tunnel definition database, wherein a remote ID in said tunnel definition is defined as said group name, wherein said server node has a single tunnel definition for each of the plurality of tunnels associated with said group name; wherein a particular tunnel of said plurality of tunnels associated with said group name is activated, wherein said particular tunnel is associated with a particular member of said group name; wherein activating said particular tunnel comprises the steps of: sending a security policy stored in a policy database of said client node by said client node to said server node; sending a security policy stored in a policy database of said server node by said server node to said client node if said security policy stored in said policy database of said server node agrees on the same set of protection suites at any point in time with said security

policy stored in said policy database of said client node; sending a first nonce by said client node to said server node; sending a second nonce by said server node to said client node; sending a first ID by said client node to said server node; and sending a second ID by said server node to said client node.

Examiner's Statement of Reasons for Allowance

2. Claims 1,2,5-48,51-70 are allowed over prior art.

3. This action is in reply to applicant's correspondence of 16 June 2004.

4. The following is an examiner's statement of reasons for the indication of allowable claimed subject matter.

5. As per claims 1,19,24,25,41,46,47,65,70, prior art of record, Bots et al, U.S. Patent 6,226,748 B1, and Shrader, U.S. Patent 5,864,666, fails to teach, alone, or in combination, of;

(claim 1) "A method for allowing a server node in a virtual private network to have a single tunnel definition and a single security policy for a plurality of tunnels associated with a group name comprising the steps of: configuring a group database in said server node, wherein said group database in said server node comprises said group name and a list of members associated with said group name; configuring a rules database in said server node, wherein said rules database associates said group name with a particular security policy, wherein said server node has a single security policy for each of the plurality of tunnels associated with said group name; establishing a tunnel having a tunnel definition between a client node having a member name and said server node by negotiating a common security policy; and *associating said tunnel with a group in said group database based on said member name such that only one copy of said*

database based on said tunnel definition and associated security policy is maintained on said server node regardless of the number of client nodes to server nod tunnels associated with said group.", and;

(claim 19) "A method for allowing a server node in a virtual private network to have a single tunnel definition and a single security policy for a plurality of tunnels associated with a group name comprising the steps of: configuring a group database in said server node, wherein said group database in said server node comprises said group name and a list of members associated with said group name; configuring a rules database in said server node, wherein said rules database associates said group name with a particular security policy, wherein said server node has a single security policy for each of the plurality of tunnels associated with said group name; establishing a tunnel having a tunnel definition between a client node having a member name and said server node by negotiating a common security policy; and *associating said tunnel with a group in said group database based on said member name such that only one copy of said database based on said tunnel definition and associated security policy is maintained on said server node regardless of the number of client nodes to server nod tunnels associated with said group*; and activating said tunnel, wherein activating said tunnel comprises the steps of sending a security policy stored in a policy database of said client node by said client node to said server node; sending a security policy stored in a policy database of said server node by said server node to said client node if said security policy stored in said policy database of said server node matches said security policy stored in said policy database of said client node; sending a first nonce by said client node to said server node; sending a second nonce by said server node to said

client node; sending a first ID by said client node to said server node; and sending a second ID by said server node to said client node.", and;

(claim 24) "A method for allowing a server node in a virtual private network to have a single tunnel definition and a single security policy for a plurality of tunnels associated with a group name comprising the steps of: configuring a group database in said server node, wherein said group database in said server node comprises said group name and a list of members associated with said group name; configuring a rules database in said server node, wherein said rules database associates said group name with a particular security policy, wherein said server node has a single security policy for each of the plurality of tunnels associated with said group name; establishing a tunnel having a tunnel definition between a client node having a member name and said server node by negotiating a common security policy; and *associating said tunnel with a group in said group database based on said member name such that only one copy of said database based on said tunnel definition and associated security policy is maintained on said server node regardless of the number of client nodes to server nod tunnels associated with said group*; and activating said tunnel, wherein activating said tunnel comprises the steps of: sending a security policy stored in a policy database of said client node by said client node to said server node; sending a security policy stored in a policy database of said server node by said server node to said client node if said security policy stored in said policy database of said server node agrees on the same set of protection suites at any point in time with said security policy stored in said policy database of said client node; sending a first nonce by said client node to said server node; sending a second nonce by said server node to said client node; sending a first ID by said

client node to said server node; and sending a second ID by said server node to said client node.", and;

(claim 25) "A virtual private network system comprising: a plurality of tunnels associated with a group name, wherein each of said plurality of tunnels associated with said group name comprises a plurality of nodes, wherein each of said plurality of nodes comprises a communication adapter to interconnect with said virtual private network, wherein one of said plurality of nodes is a server node, wherein one of said plurality of nodes is a client node, wherein said server node comprises: a group database, wherein said group database comprises said group name and a list of members associated with said group name; and a rules database, wherein said rules database associates said group name with a particular security policy, wherein said *server node has a single copy of a security policy for each of the plurality of tunnels associated with said group name*.", and;

(claim 41) "A virtual private network system comprising: a plurality of tunnels associated with a group name, wherein each of said plurality of tunnels associated with said group name comprises a plurality of nodes, wherein each of said plurality of nodes comprises a communication adapter to interconnect with said virtual private network, wherein one of said plurality of nodes is a server node, wherein one of said plurality of nodes is a client node, wherein said server node comprises: a group database, wherein said group database comprises said group name and a list of members associated with said group name; and a rules database, wherein said rules database associates said group name with a particular security policy, wherein said *server node has a single copy of a security policy for each of the plurality of tunnels associated with said group name*; wherein the server node further comprises; a tunnel definition

database, wherein a remote ID in said tunnel definition is defined as said group name, wherein said server node has a single tunnel definition for each of the plurality of tunnels associated with said group name; wherein a particular tunnel of said plurality of tunnels associated with said group name is activated, wherein said particular tunnel is associated with a particular member of said group name; wherein activating said particular tunnel comprises the steps of: sending a security policy stored in a policy database of said client node by said client node to said server node; sending a security policy stored in a policy database of said server node by said server node to said client node if said security policy stored in said policy database of said server node **matches** said security policy stored in said policy database of said client node; sending a first nonce by said client node to said server node; sending a second nonce by said server node to said client node; sending a first ID by said client node to said server node; and sending a second ID by said server node to said client node.", and;

(claim 46) "A virtual private network system comprising: a plurality of tunnels associated with a group name, wherein each of said plurality of tunnels associated with said group name comprises a plurality of nodes, wherein each of said plurality of nodes comprises a communication adapter to interconnect with said virtual private network, wherein one of said plurality of nodes is a server node, wherein one of said plurality of nodes is a client node, wherein said server node comprises: a group database, wherein said group database comprises said group name and a list of members associated with said group name; and a rules database, wherein said rules database associates said group name with a particular security policy, wherein said *server node has a single copy of a security policy for each of the plurality of tunnels associated with said group name*; wherein the server node further comprises; a tunnel definition

database, wherein a remote ID in said tunnel definition is defined as said group name, wherein said server node has a single tunnel definition for each of the plurality of tunnels associated with said group name; wherein a particular tunnel of said plurality of tunnels associated with said group name is activated, wherein said particular tunnel is associated with a particular member of said group name; wherein activating said particular tunnel comprises the steps of: sending a security policy stored in a policy database of said client node by said client node to said server node; sending a security policy stored in a policy database of said server node by said server node to said client node if said security policy stored in said policy database of said server node **agrees on the same set of protection suites at any point in time** with said security policy stored in said policy database of said client node; sending a first nonce by said client node to said server node; sending a second nonce by said server node to said client node; sending a first ID by said client node to said server node; and sending a second ID by said server node to said client node.", and;

(claim 47) "A computer program product having a computer readable medium having computer program logic recorded thereon for allowing a server node in a virtual private network to have a single tunnel definition and a single security policy for a plurality of tunnels associated with a group name, comprising: programming operable for configuring a group database in said server node, wherein said group database in said server node comprises said group name and a list of members associated with said group name; programming operable for configuring a rules database in said server node, wherein said rules database associates said group name with a particular security policy, wherein said server node has a single security policy for each of the plurality of tunnels associated with said group name; programming operable for establishing a

tunnel having a tunnel definition between a client node having a member name and said server node by negotiating a common security policy; and programming operable for *associating said tunnel with a group in said group database based on said member name such that only one copy of said database based on said tunnel definition and associated security policy is maintained on said server node regardless of the number of client nodes to server nod tunnels associated with said group*.", and;

(claim 65) "A computer program product having a computer readable medium having computer program logic recorded thereon for allowing a server node in a virtual private network to have a single tunnel definition and a single security policy for a plurality of tunnels associated with a group name, comprising: programming operable for configuring a group database in said server node, wherein said group database in said server node comprises said group name and a list of members associated with said group name; programming operable for configuring a rules database in said server node, wherein said rules database associates said group name with a particular security policy, wherein said server node has a single security policy for each of the plurality of tunnels associated with said group name; programming operable for establishing a tunnel having a tunnel definition between a client node having a member name and said server node by negotiating a common security policy; and programming operable for *associating said tunnel with a group in said group database based on said member name such that only one copy of said database based on said tunnel definition and associated security policy is maintained on said server node regardless of the number of client nodes to server nod tunnels associated with said group*; and programming operable for activating said tunnel, wherein said programming operable for activating said tunnel comprises: programming operable for of sending a security

policy stored in a policy database of said client node by said client node to said server node; programming operable for sending a security policy stored in a policy database of said server node by said server node to said client node if said security policy stored in said policy database of said server node matches said security policy stored in said policy database of said client node; programming operable for sending a first nonce by said client node to said server node; programming operable for sending a second nonce by said server node to said client node; programming operable for sending a first ID by said client node to said server node; and programming operable for sending a second ID by said server node to said client node.", and;

(claim 70) "A computer program product having a computer readable medium having computer program logic recorded thereon for allowing a server node in a virtual private network to have a single tunnel definition and a single security policy for a plurality of tunnels associated with a group name, comprising: programming operable for configuring a group database in said server node, wherein said group database in said server node comprises said group name and a list of members associated with said group name; programming operable for configuring a rules database in said server node, wherein said rules database associates said group name with a particular security policy, wherein said server node has a single security policy for each of the plurality of tunnels associated with said group name; programming operable for establishing a tunnel having a tunnel definition between a client node having a member name and said server node by negotiating a common security policy; and programming operable for *associating said tunnel with a group in said group database based on said member name such that only one copy of said database based on said tunnel definition and associated security policy is maintained on said server node regardless of the number of client nodes to server nod tunnels associated with*

said group; and programming operable for activating said tunnel, wherein said programming operable for activating said tunnel comprises: programming operable for of sending a security policy stored in a policy database of a client node by said client node to said server node; programming operable for sending a security policy stored in a policy database of said server node by said server node to said client node if said security policy stored in said policy database of said server node agrees on the same set of protection suites at any point in time with said security policy stored in said policy database of said client node; programming operable for sending a first nonce by said client node to said server node; programming operable for sending a second nonce by said server node to said client node; programming operable for sending a first 1D by said client node to said server node; and programming operable for sending a second ID by said server node to said client node.".

The *italicized* above claim elements dealing with "*associating said tunnel with a group in said group database based on said member name such that only one copy of said database based on said tunnel definition and associated security policy is maintained on said server node regardless of the number of client nodes to server nod tunnels associated with said group*" and "*server node has a single copy of a security policy for each of the plurality of tunnels associated with said group name"* serving to patently distinguish the invention from prior art. Specifically, the use of VPN client/server elements having associated distributed databases defining the tunnels and associated security policies is taught in the prior art. However, as per the applicants arguments in the previous remarks in Amendment A (February 20, 2004), the examiner finds the applicant's arguments to be persuasive in that; "Bots does not disclose '*associating said tunnel with ... only one copy of said database ... with said group*' as recited in claim 1...".

Dependent claims 2,5-18,20-23,26-40,42-45,48,51-64,66-69 are allowable by virtue of their dependencies.

Conclusion

6. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (703) 305-4276. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The Fax number for the organization where this application is assigned is 703-872-9306.

Ronald Baum

Patent Examiner

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100